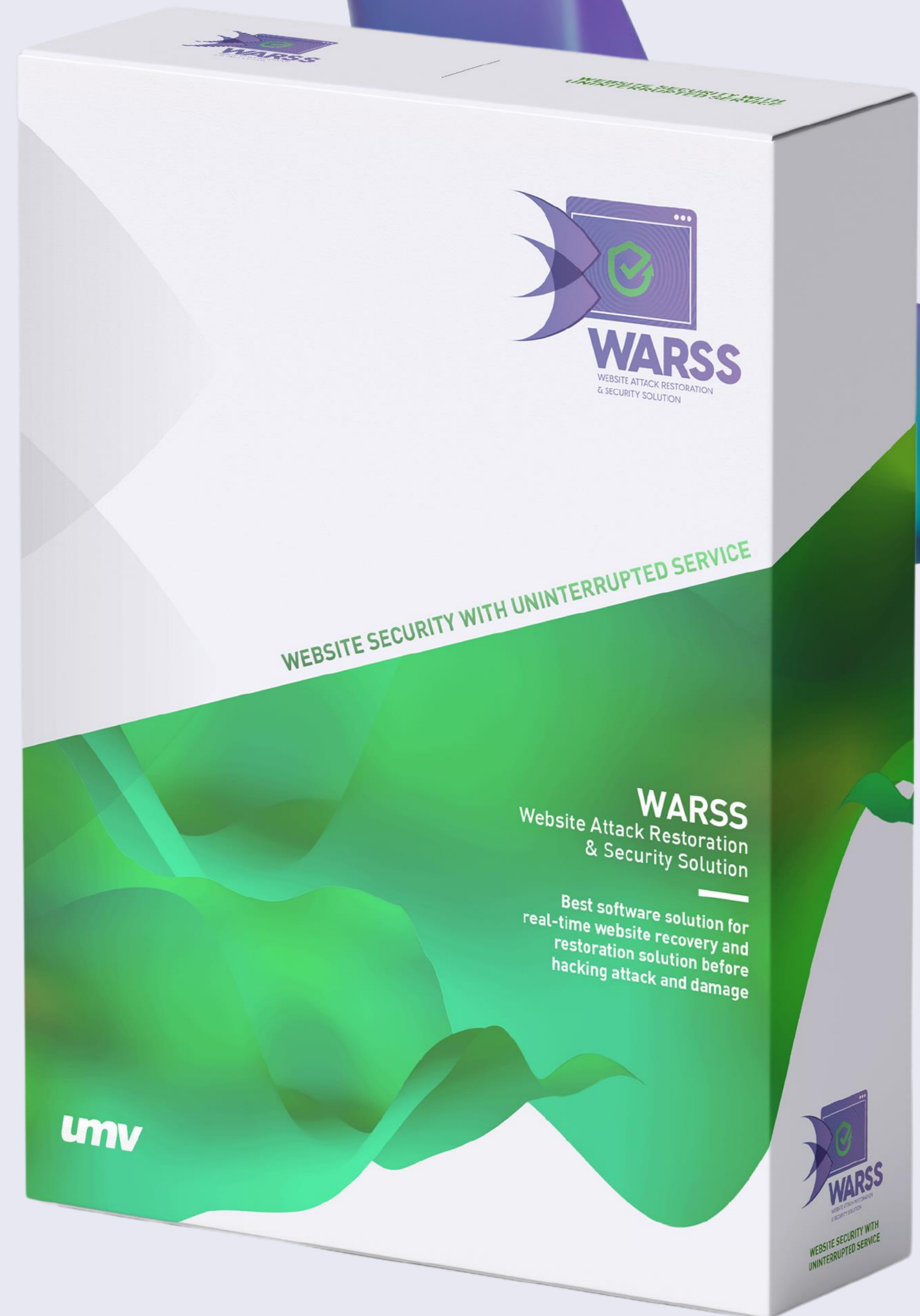




# WARSS

## Website Attack Restoration Security Solution

Защита веб-сайта в режиме реального времени



# Содержание

**01**

**О нас**

**02**

**Тенденции в  
области веб-  
хакинга**

**03**

**Проблема**

**04**

**WARSS**

**05**

**Примеры  
использования**

**06**

**Вопросы и  
ответы**

# umv



## UMV Inc.

**Основана в 2008 году**

Сеул, Южная Корея

**Веб-ориентированные решения**

Безопасность веб-сервера в режиме реального времени

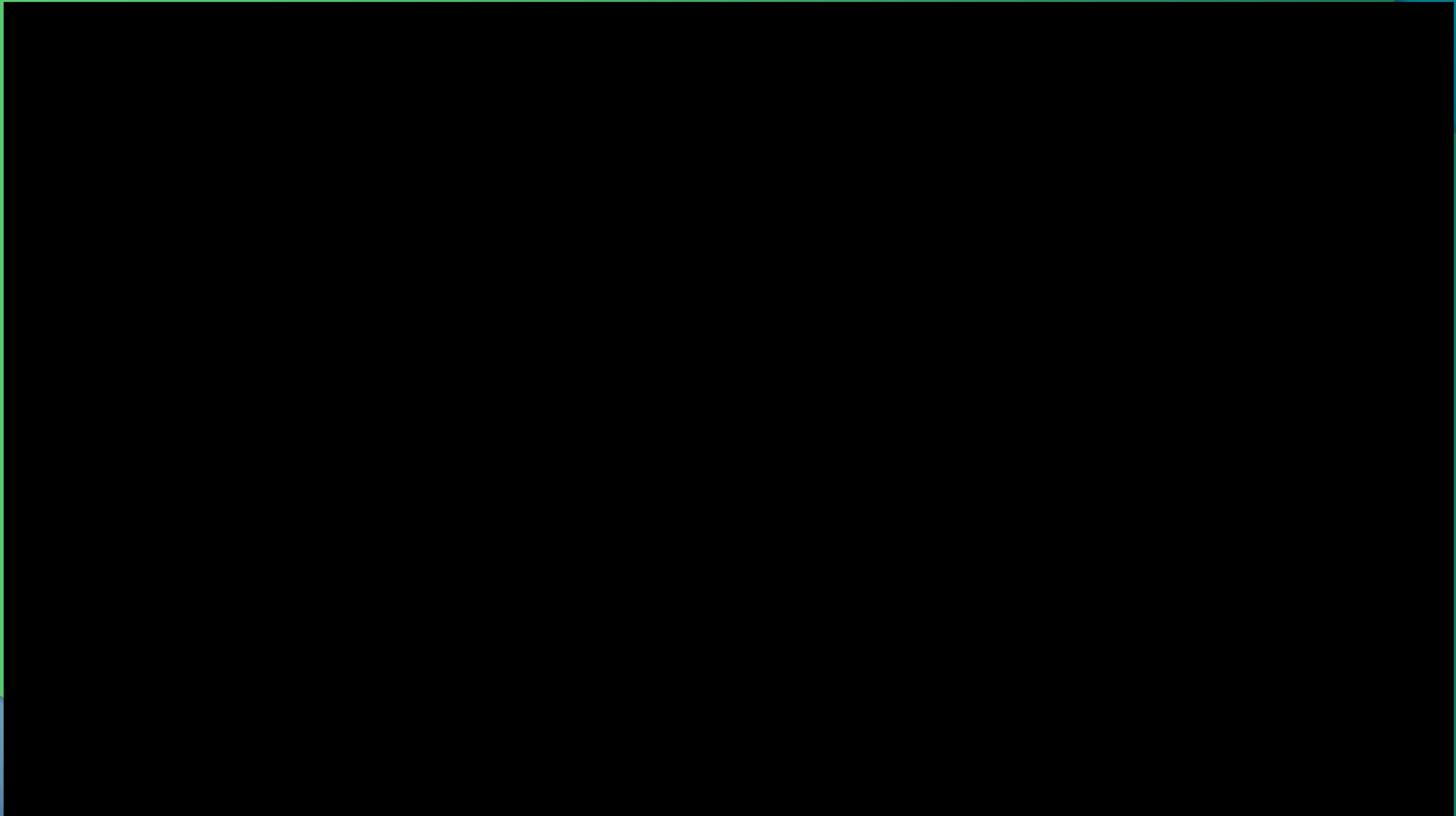
**Предотвратить**

Кража данных, прерывание работы веб-сервисов, порча веб-сайтов, постоянные атаки

**Девиз**

«Цепь безопасности сильна лишь настолько, насколько сильно ее самое слабое звено»

# Почему WARSS?



<https://www.youtube.com/watch?v=6gY1NWw9CJA&t=12s>

# Веб-хакерство набирает обороты

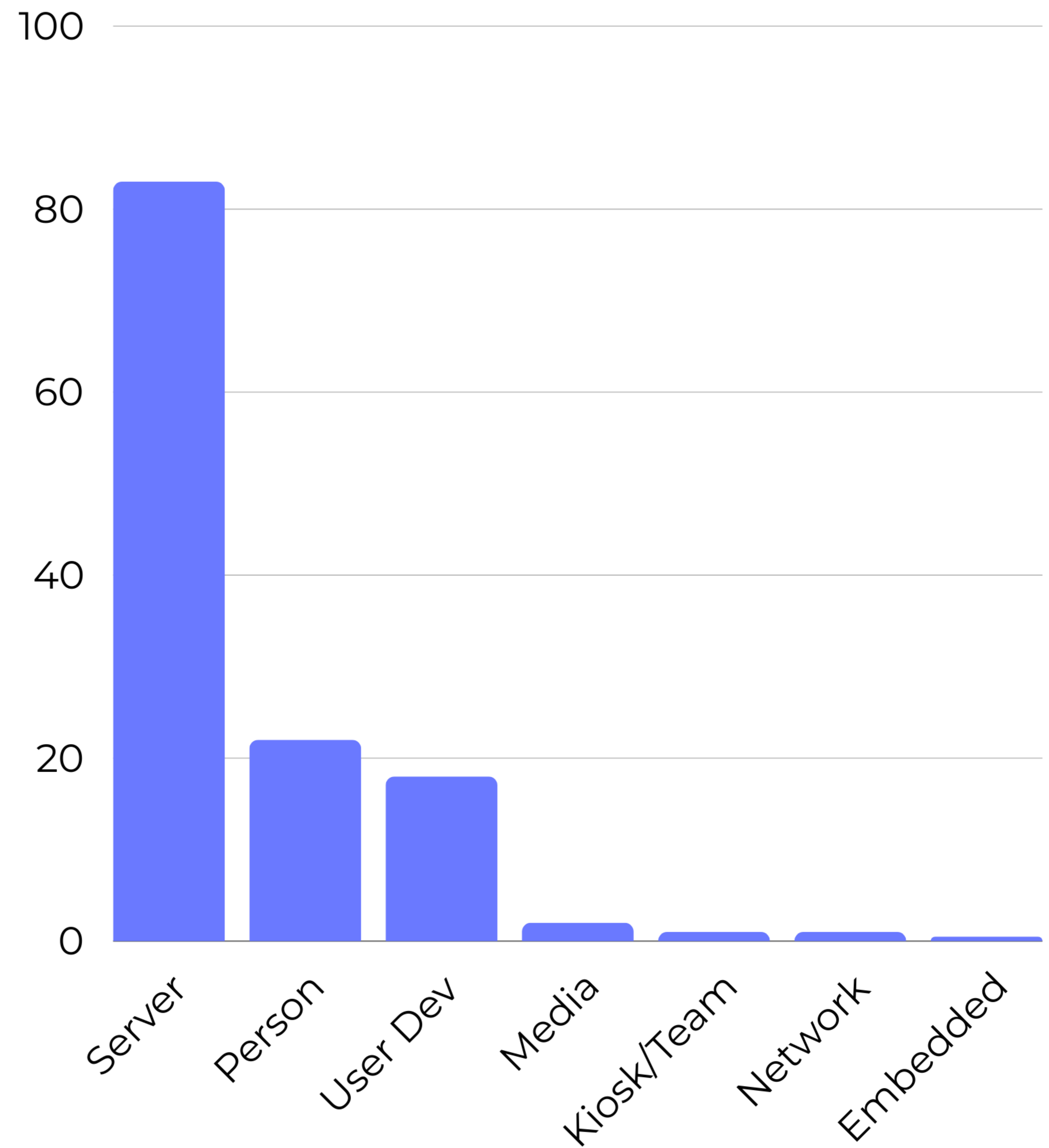


Verizon проанализировал рекордный **двухкратный** рост числа подтвержденных **нарушений безопасности** в период с 2022 по 2023 год.

Отчет о расследовании утечки данных Verizon за 2024 год

# Активы, пострадавшие в результате нарушений

2023 Verizon DBIR



# Взломаны украинские и российские сайты

## Поддельные новости

Февраль 2024 г. — настоящее время:

Российско-украинская война сопровождается постоянными кибератаками друг на друга и союзников

## Дезинформация и сбор данных

Целями являются предприятия малого и среднего бизнеса, средства массовой информации, государственные учреждения, ОТ и другие организации, обладающие личной/конфиденциальной информацией.

## Недоверие: Ключ к кибервойнам

Публичность хакерских атак порождает страх, недоверие к властям и дезинформацию среди гражданского населения

**BREAKING**

[Image Source: The Record](#)

## PERVOKLASSNIY RUSSIAN HACKERS ATTACK

11 mins ago

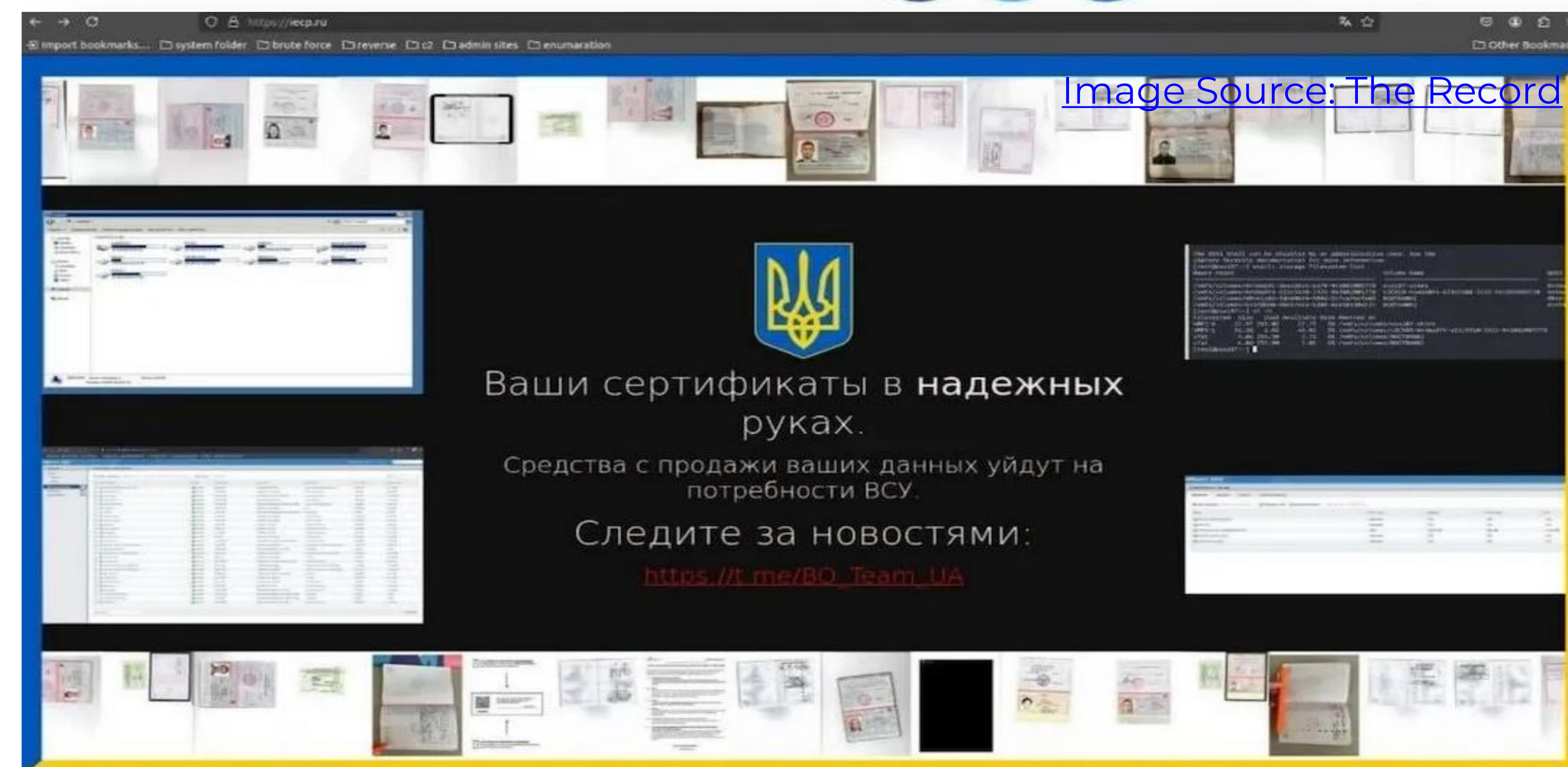
CHARITY COURT CRIME ECONOMY EDUCATION



By Дэниел Хопкинс

Share No Comments

[Image Source: The Record](#)



# Атаки на Интернет-архив

## Раунд 1: DDoS-атака, порча интерфейса, кража данных

9 октября 2024 года: DDoS-атака выводит сайт из строя; веб-сайт подвергся порче с использованием JavaScript-уведомления; имена пользователей, электронные адреса и другие данные 31 миллиона учетных записей утекли

## Обратно к первоначальному виду

18 октября 2024 года: IA подтверждает, что данные в безопасности и услуги восстановлены

## Раунд 2: Не защищенные цифровые ключи

20 октября 2024 года: Использование не обновленных токенов доступа для получения доступа к платформе поддержки Zendesk Интернет-архива; доступ к более чем 800 тыс. заявок в поддержку, начиная с 2018 года

[Image Source: Hack Read](#)



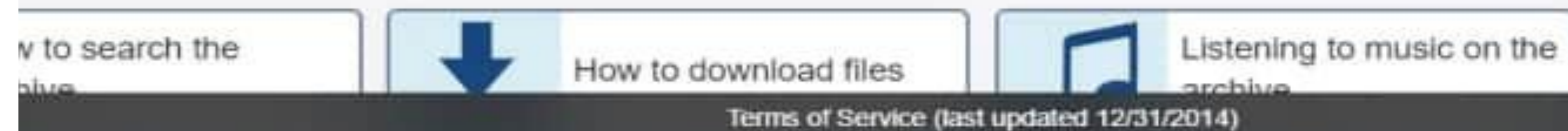
Internet Archive is a non-profit library of millions of free texts, movies, software, music, websites, and more.



Search

Advanced Se

New to the Archive?





# Тренд: Хактивизм и кибертерроризм

- Взлом с целью продвижения политических или религиозных убеждений
- Увеличенная доступность платформ для зашифрованной связи (например, Telegram, Rocket Chat, Discord и т.д.) и **криптовалют**
  - **TRON** составил **около 90% средств**, связанных с **финансированием** терроризма с 2021 года (Форум новых технологий INTERPOL, октябрь 2023 года, Merkle Science)
- **Киберпреступность как услуга** (DDoS-атаки, программное обеспечение-вымогатели, учетные данные, данные и т.д.)

- Отчет "the Surface Report" (Июнь, 2024)  
**UN Counter-Terrorism Centre (UNCCT)**



Image Source: [Malcontent News](#)



Image Source: [POLITICO](#)

# Проблема

# Методы порчи веб-сайтов

## 1. Модификация исходного кода

Bitcoin, eh? Never heard of it. But perchance you would like to try something better. Something with more "zing". Something named CosbyCoin!

Continue =>

crash.. Holding my Cosbycoin..	bitjet	2	333	Today at 07:33:43 pm by kjj
	WiseOldOwl	9	402	Today at 07:32:21 pm by ShadowOfHarbringer
iform to Mt Gox. Anybody interested? < 1	4xCoder	24	1564	Today at 07:32:20 pm by AlexZ
	mizerydeana	17	562	Today at 07:19:34 pm by ssaCEO
Image Source: alphavilleherald.com buttc01s.org		17	1501	Today at 06:58:32 pm by enmakou




**FUCK! KOREA**

Deploy the Sade missile system is ignorant  
Lotte group is too naive!  
Cherish peace, stay away from war!  
Boycott lotte, resisit Sade!  
lotte,get out of China! Korea sticks fuckyou!

犯我中华者虽远必诛!


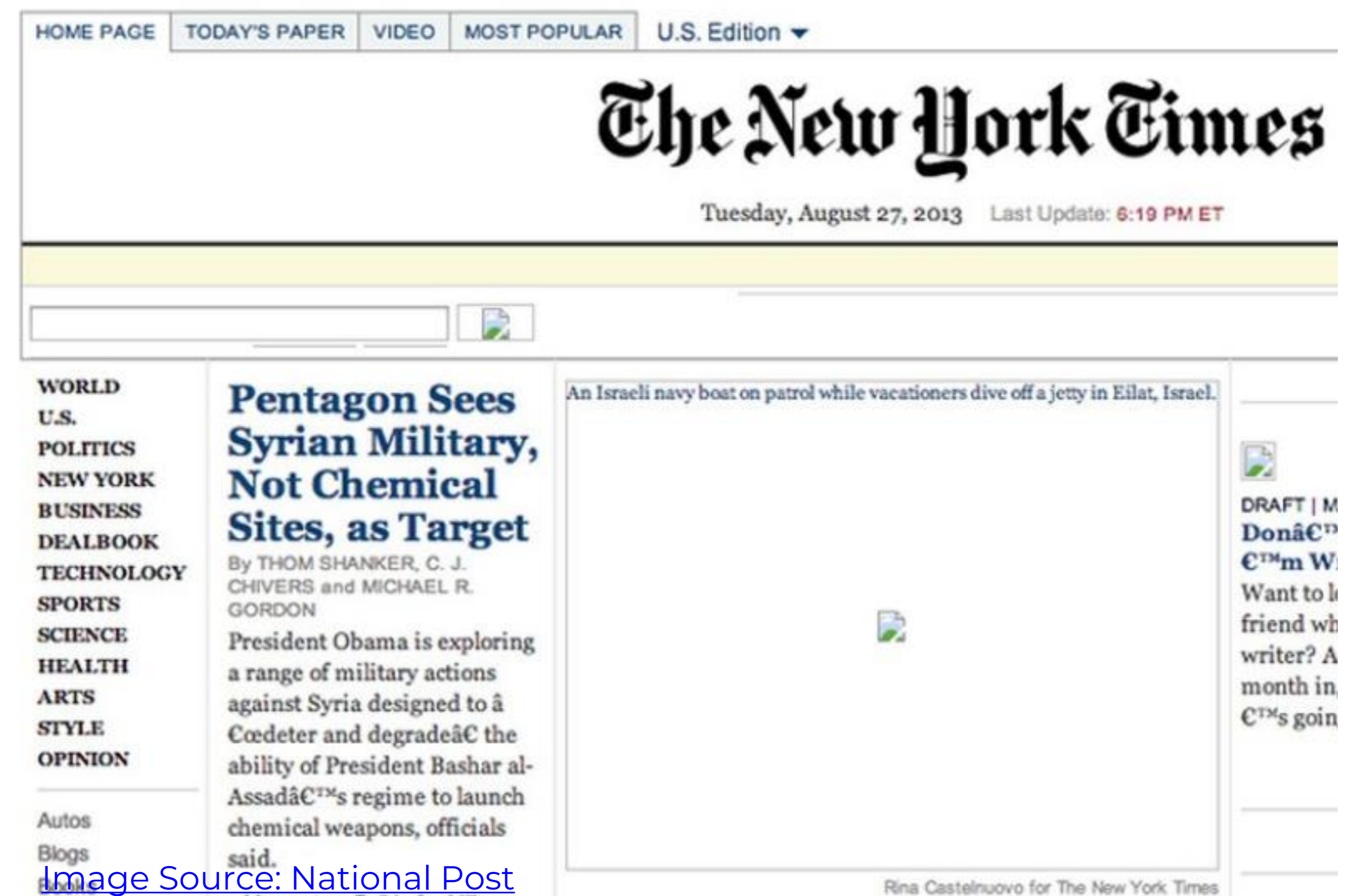
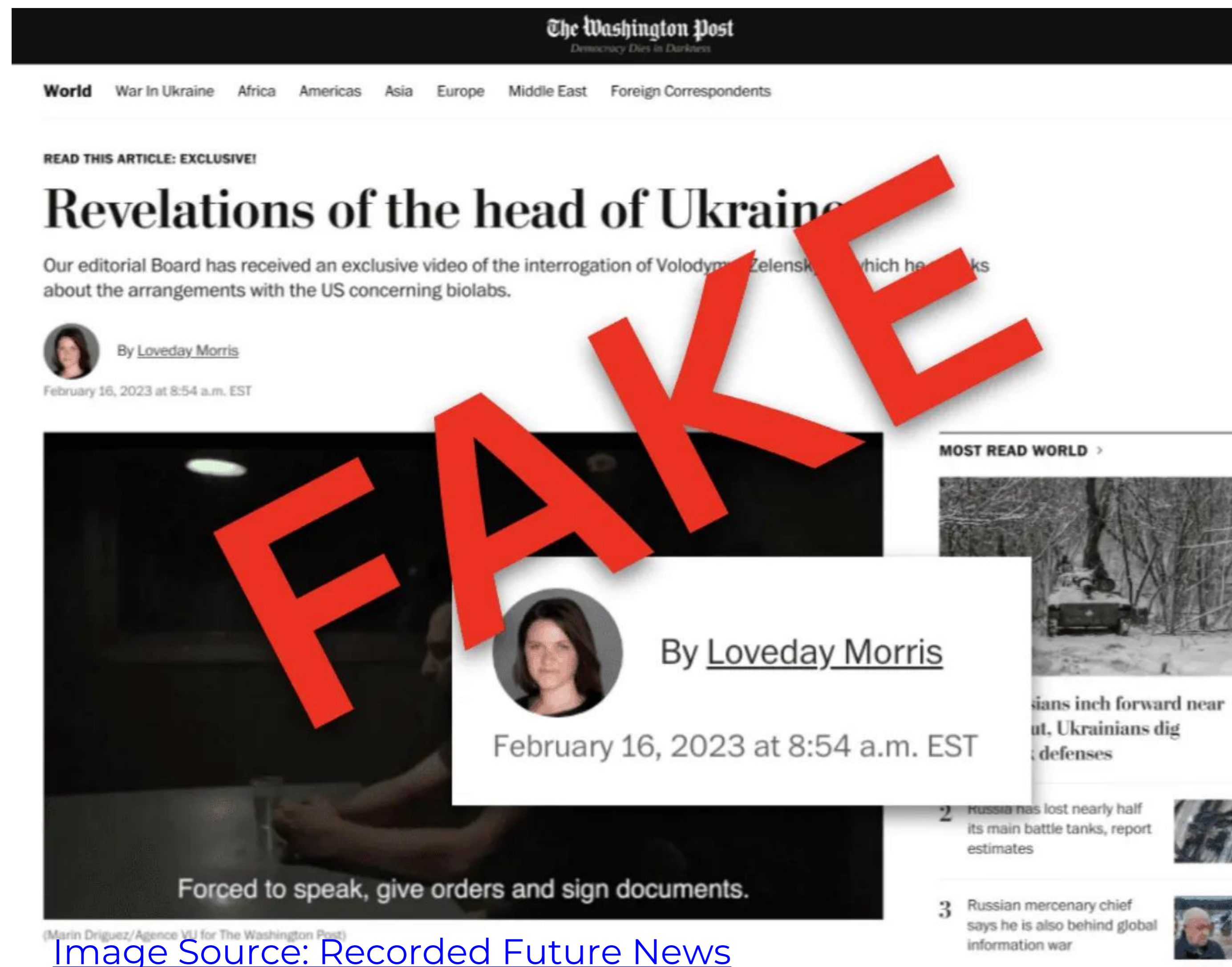


Image Source: boannews.com Intelligence Bureau

# Методы порчи веб-сайтов

## 2. Подделка контента/внедрение контента

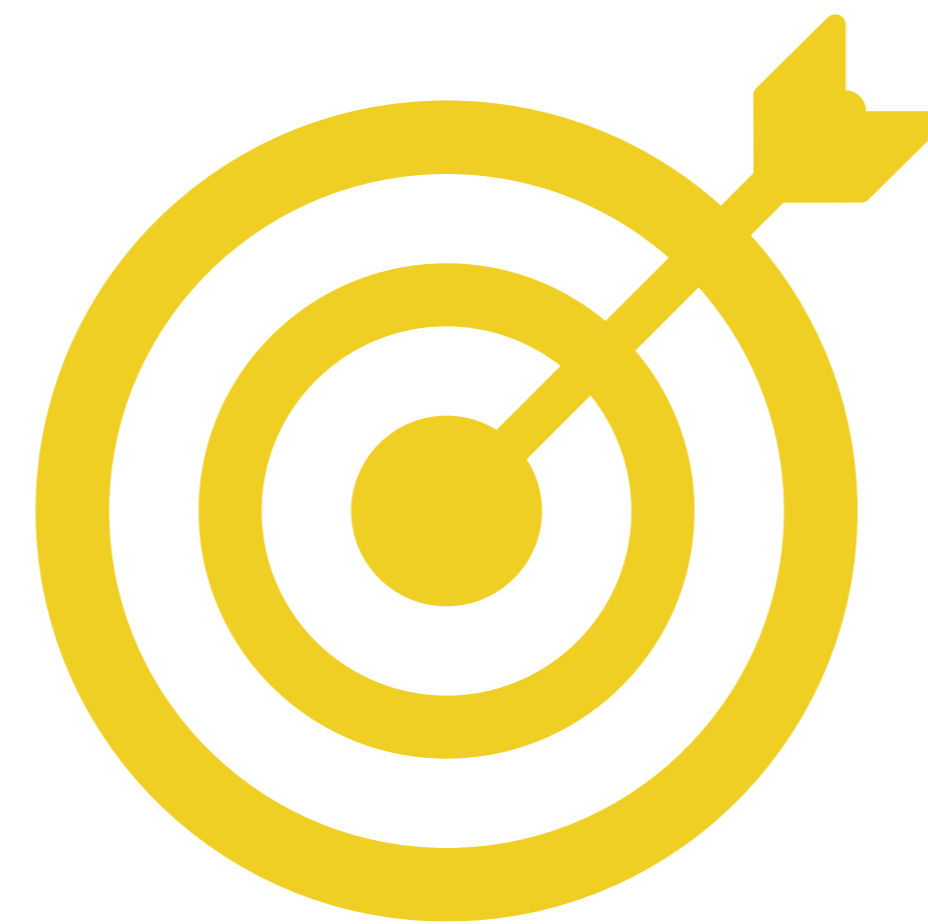


# Зачем порча веб-сайтов?



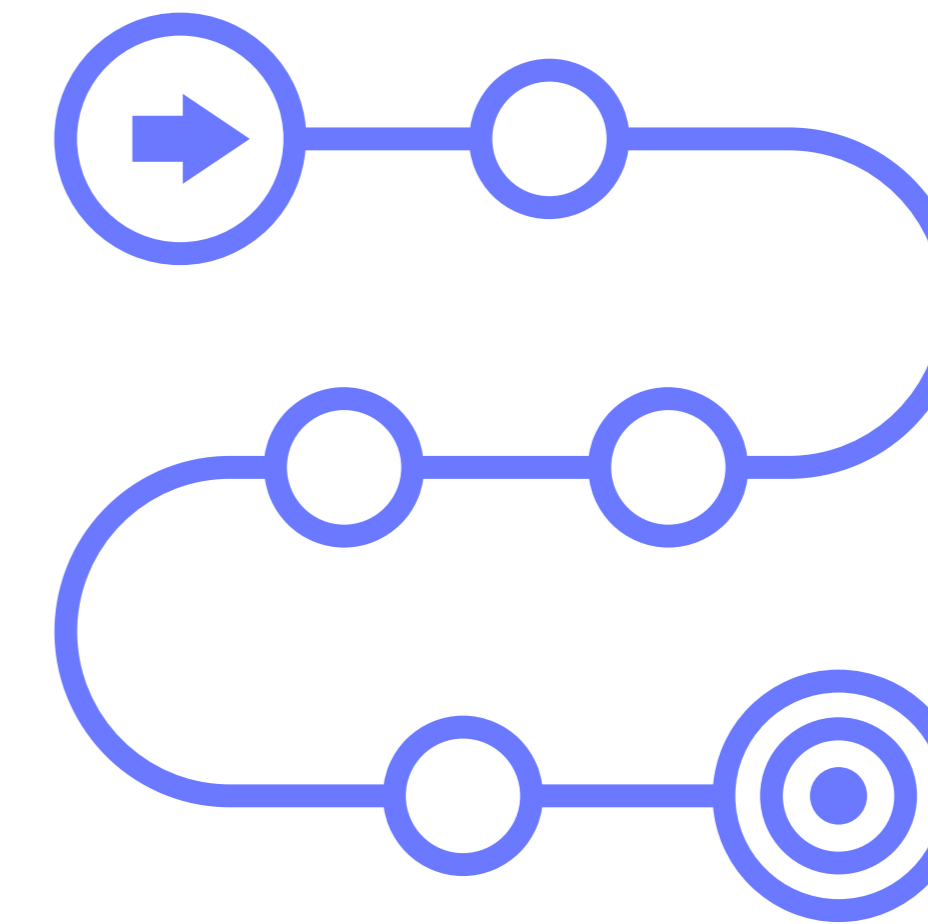
## Мотивация

- Хактивизм
- Стыд
- Слава/признание
- Кибертерроризм



## Цель

- Правительственные учреждения
- здравоохранение
- Крупные компании
- Цели удобства

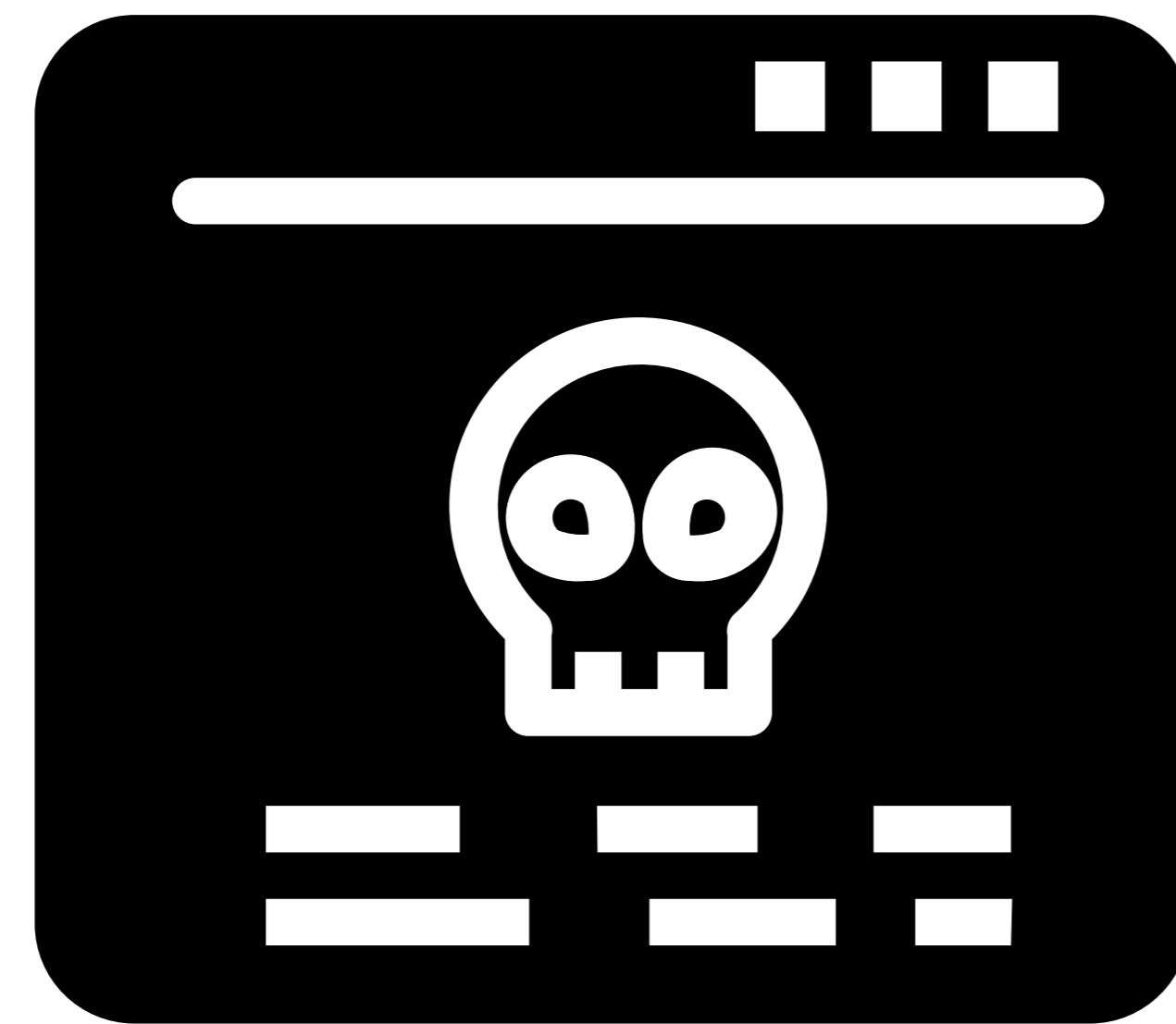
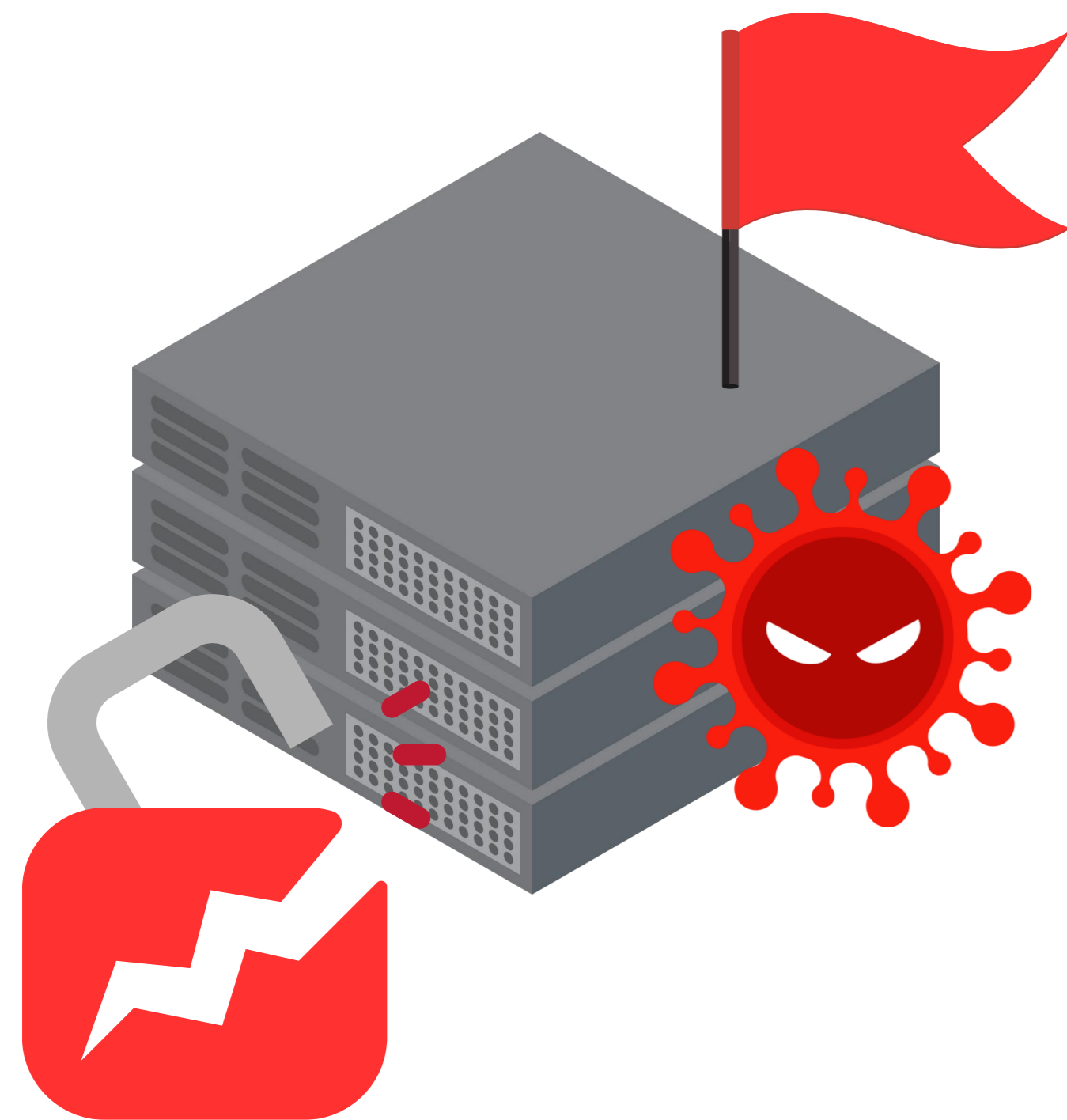


## Метод

Эксплуатация уязвимостей в веб-компонентах:

- Веб-серверы
- Веб-приложения
- Веб-сайты

# Анатомия веб-атаки



3

## Влияние

- Порча веб-сайта
- Подделка исходного кода и контента

## Эскалация

2

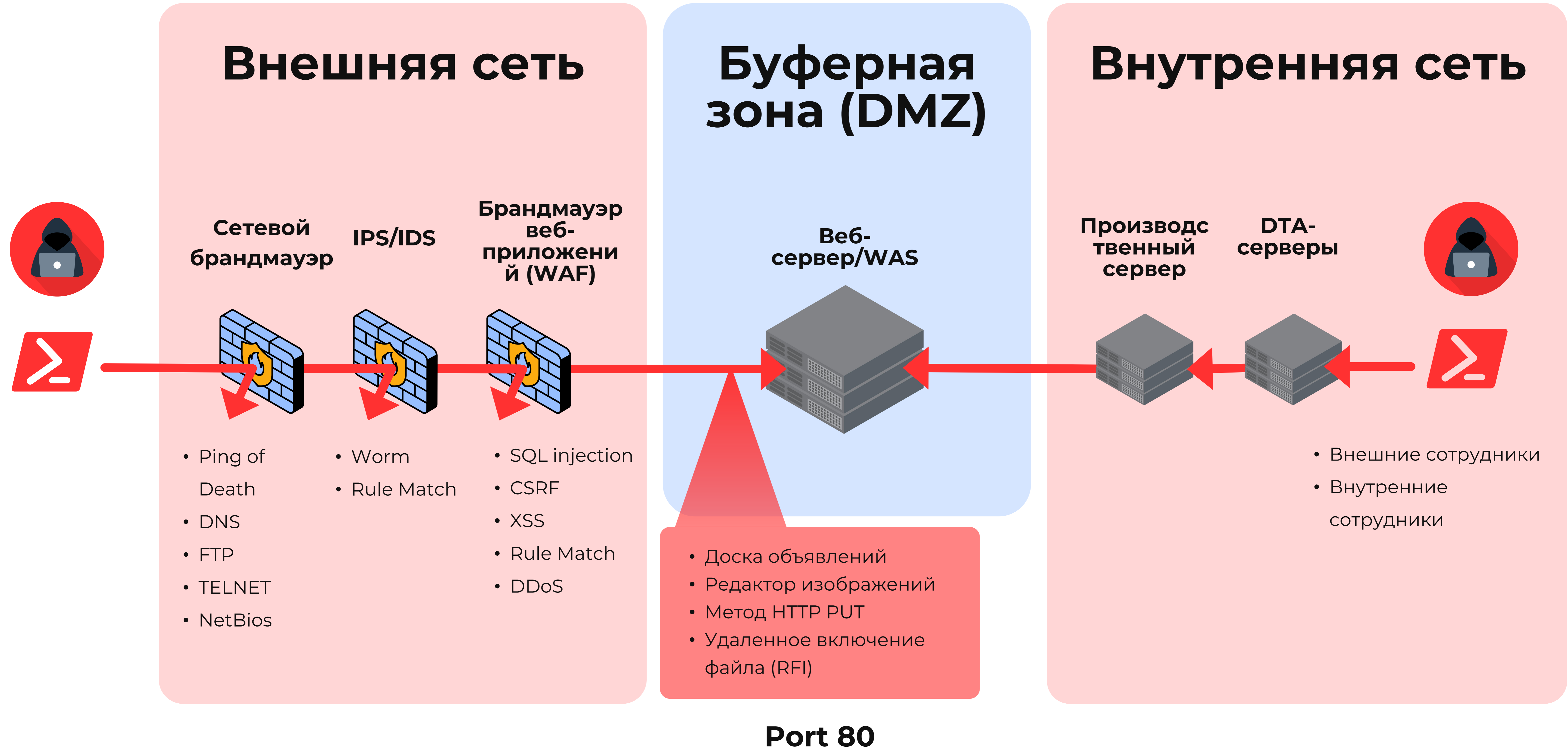
- Вредоносное ПО загружается на веб-сервер для установления присутствия
- Дополнительное вредоносное ПО (payload) выполняется для изменения файлов веб-сервера

## Проникновение

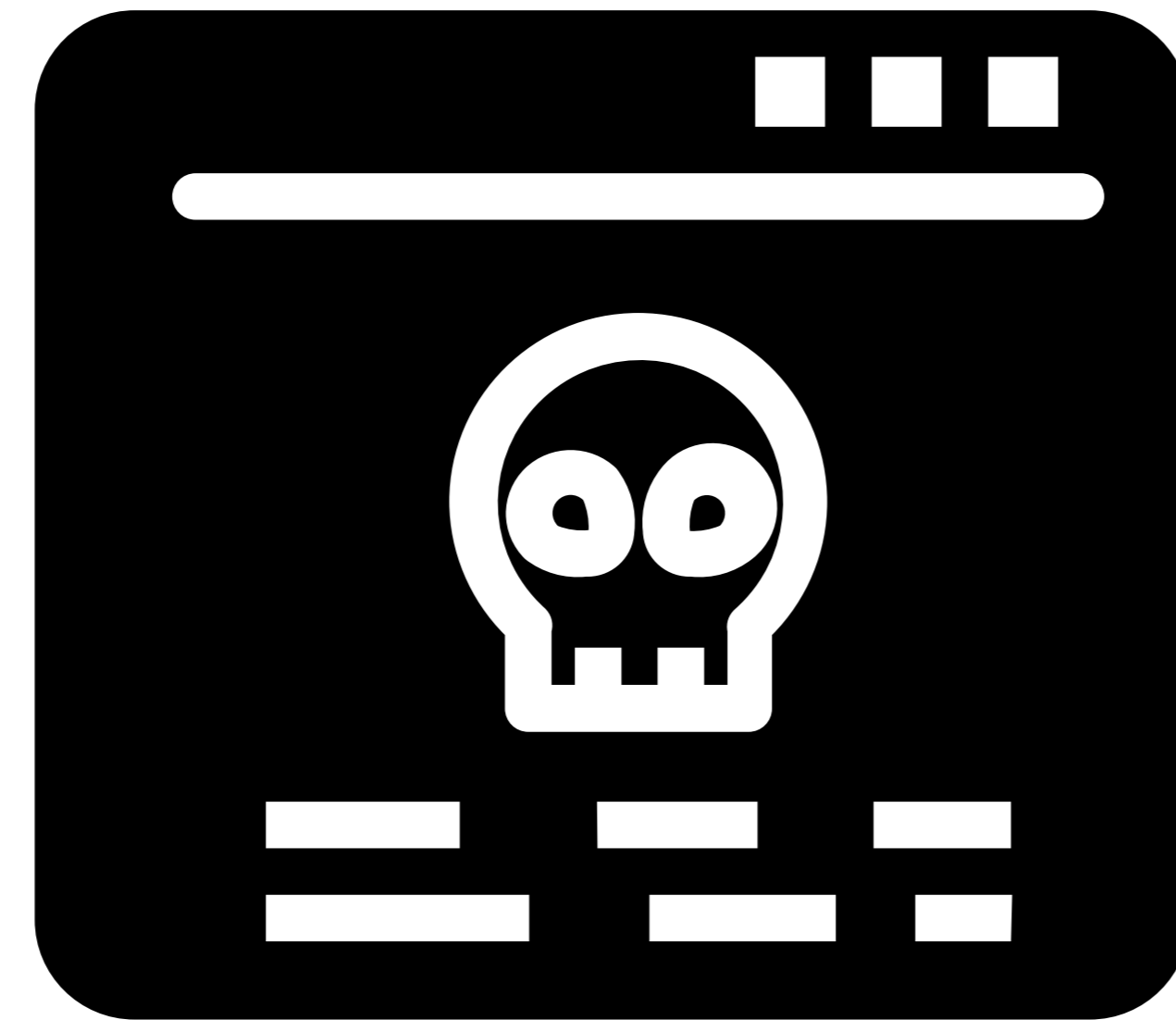
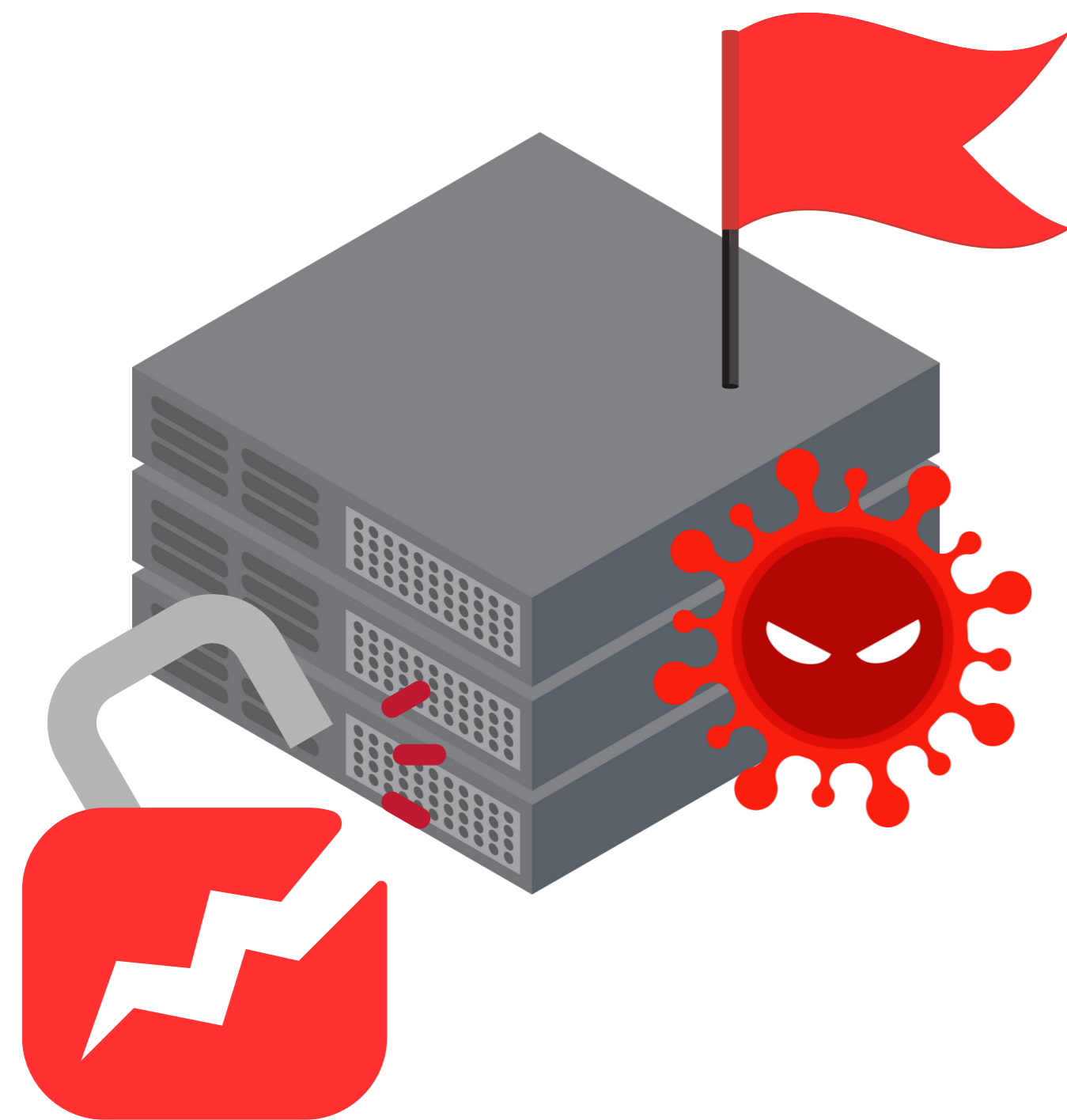
1

- Уязвимости веб-сервера или WAS используются для получения начального доступа
- Например: SQL-инъекция, украденные учетные данные, фишинг

# Статус-кво



# Анатомия веб-атаки



3

## Влияние

- Порча веб-сайта
- Подделка исходного кода и контента

## Эскалация

2

- Вредоносное ПО загружается на веб-сервер для **установления присутствия**
- Дополнительное вредоносное ПО (payload) выполняется для изменения файлов веб-сервера

## Проникновение

1

- Уязвимости веб-сервера или WAS используются для получения начального доступа
- Например: SQL-инъекция, украденные учетные данные, фишинг





Ваш сайт был взломан, не паникуйте, свяжитесь с моим адресом электронной почты, и мы решим эту проблему. Помните, даже если вы исправите ее снова, я все равно смогу получить доступ к своей оболочке backdoor, даже если вы удалили свой сайт, она не надежна.

your website has been hacked by [REDACTED], don't panic  
contact my email and we will solve it well remember  
even if you fix it again I can still access my  
shell backdor even though you have deleted your website, it is not sturdy

Contact Me [REDACTED] : [REDACTED]@gmail.com

<https://blog.sucuri.net/wp-content/uploads/2023/03/image-1.jpg>

# Ключ: Обнаружение и реагирование в режиме реального времени

Все атаки начинаются с одного из трех изменений:



**1**  
Добавление  
файла



**2**  
Изменение  
файла



**3**  
Удаление  
файлов

# Website Attack Restoration & Security Solution (WARSS)

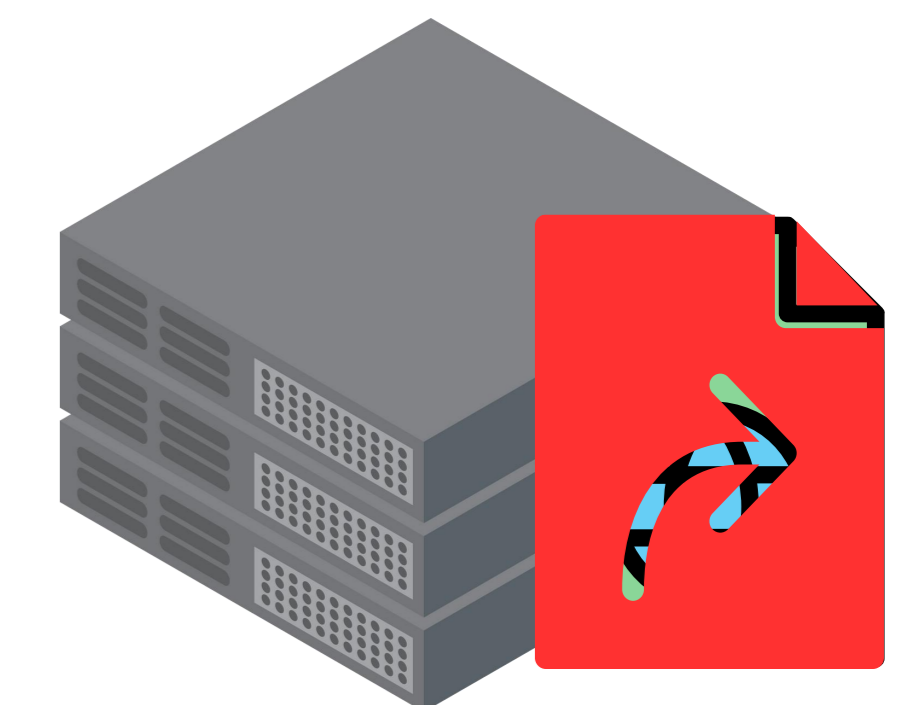
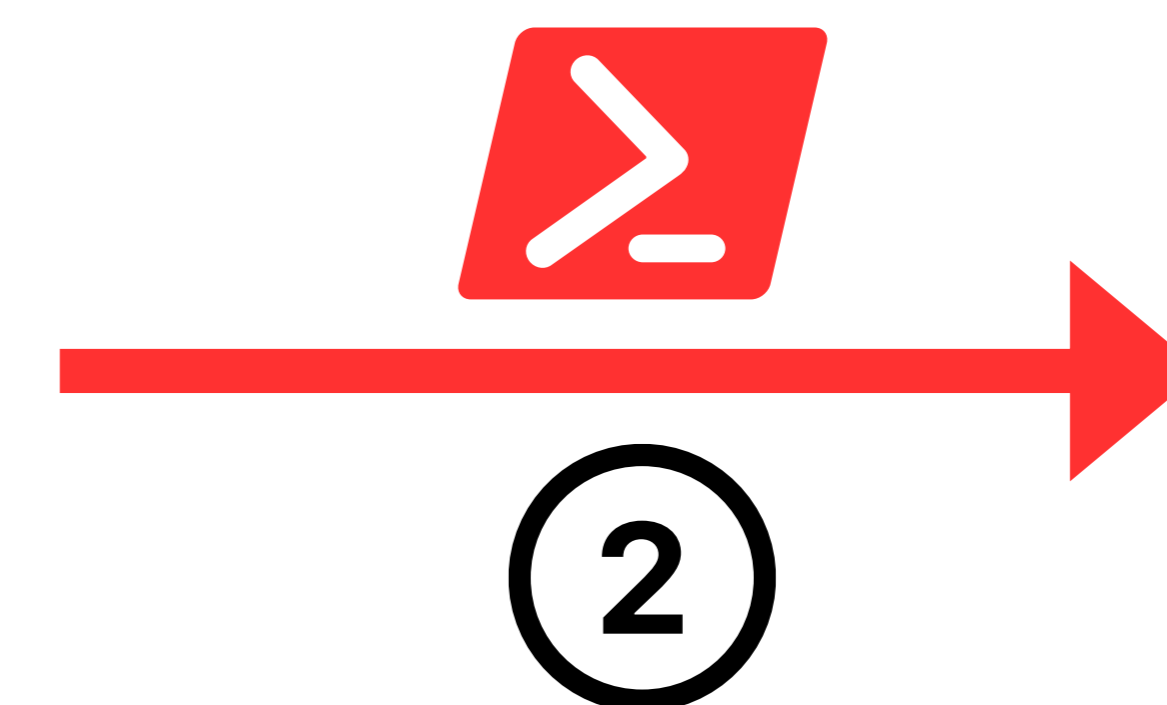
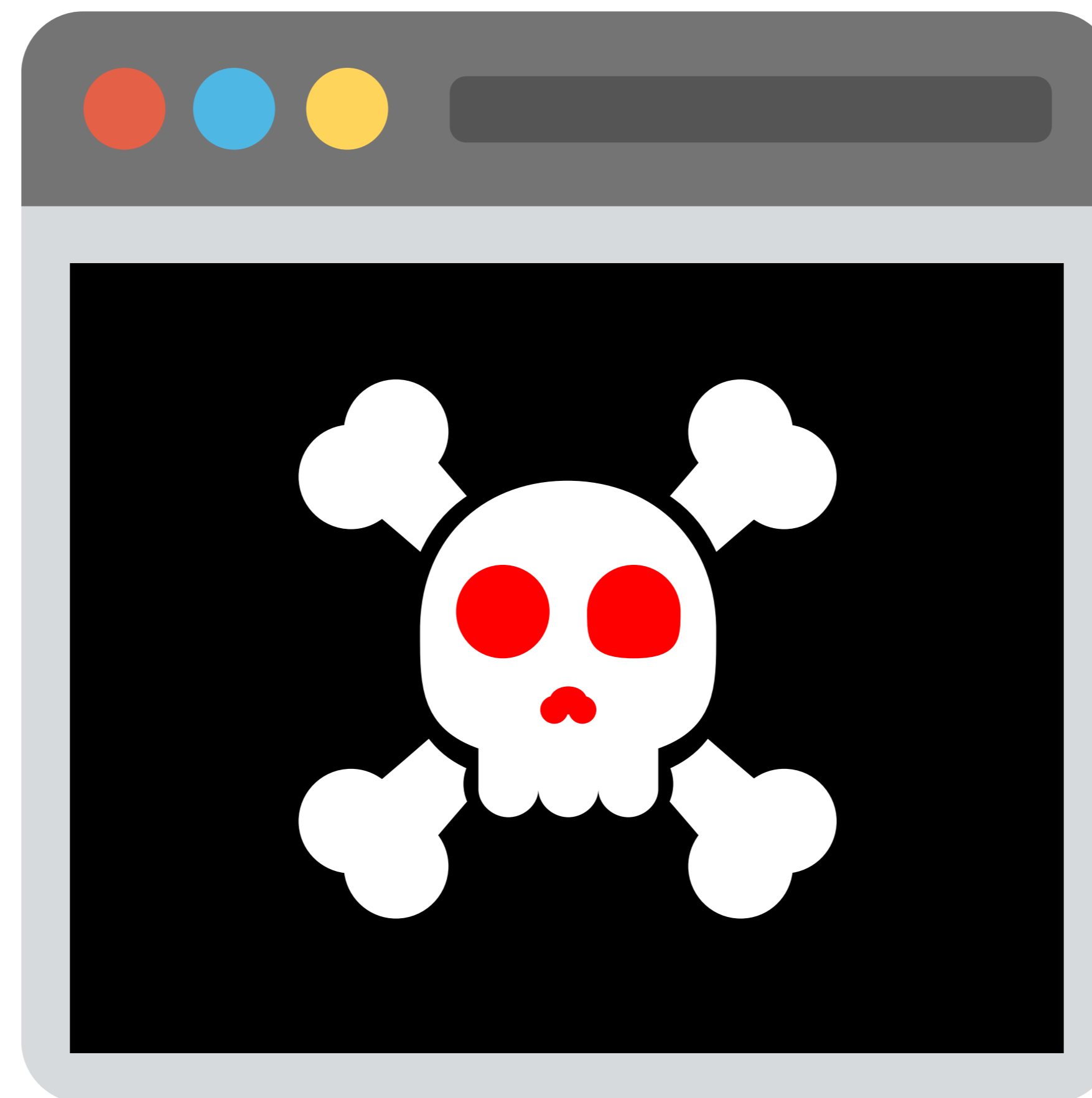
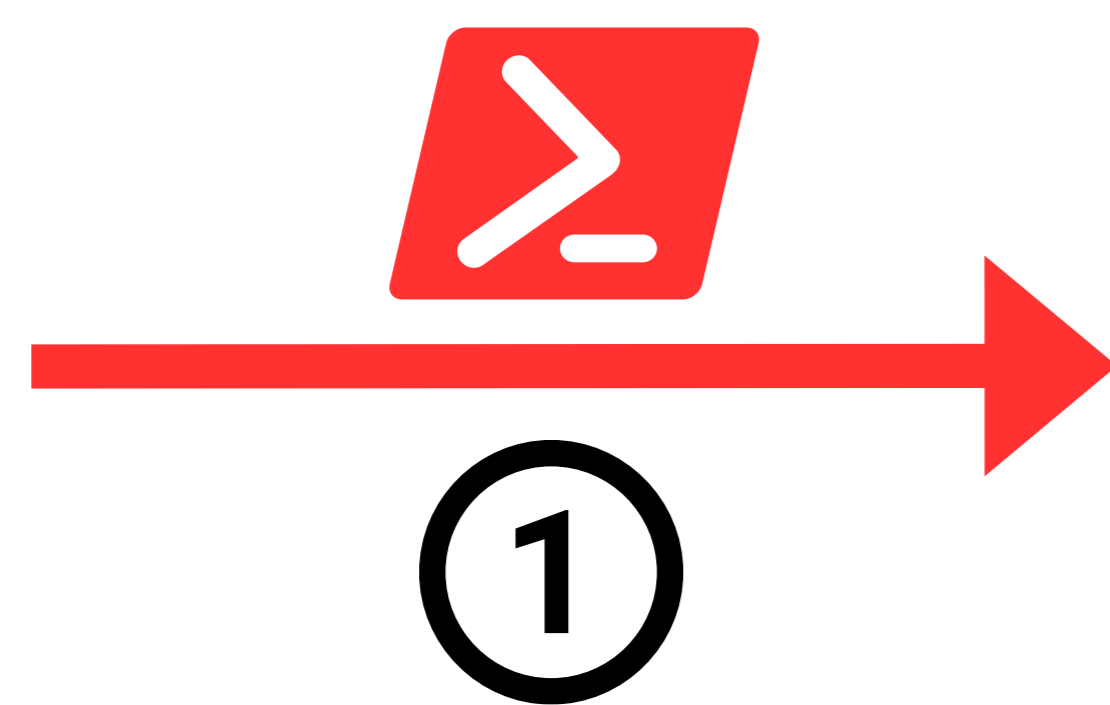
Решение для повышения безопасности веб-сервера, которое **обнаруживает** несанкционированные изменения на веб-сайте и **восстанавливает** исходные файлы в **режиме реального времени**



# Как происходит порча сайта?

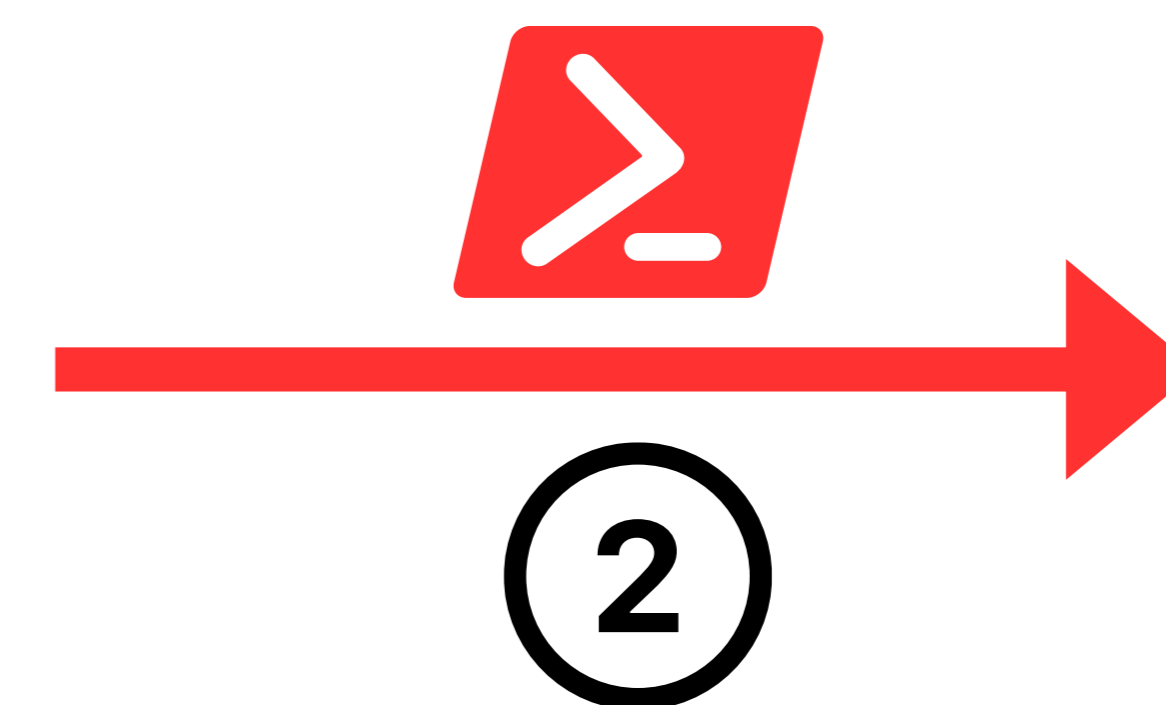
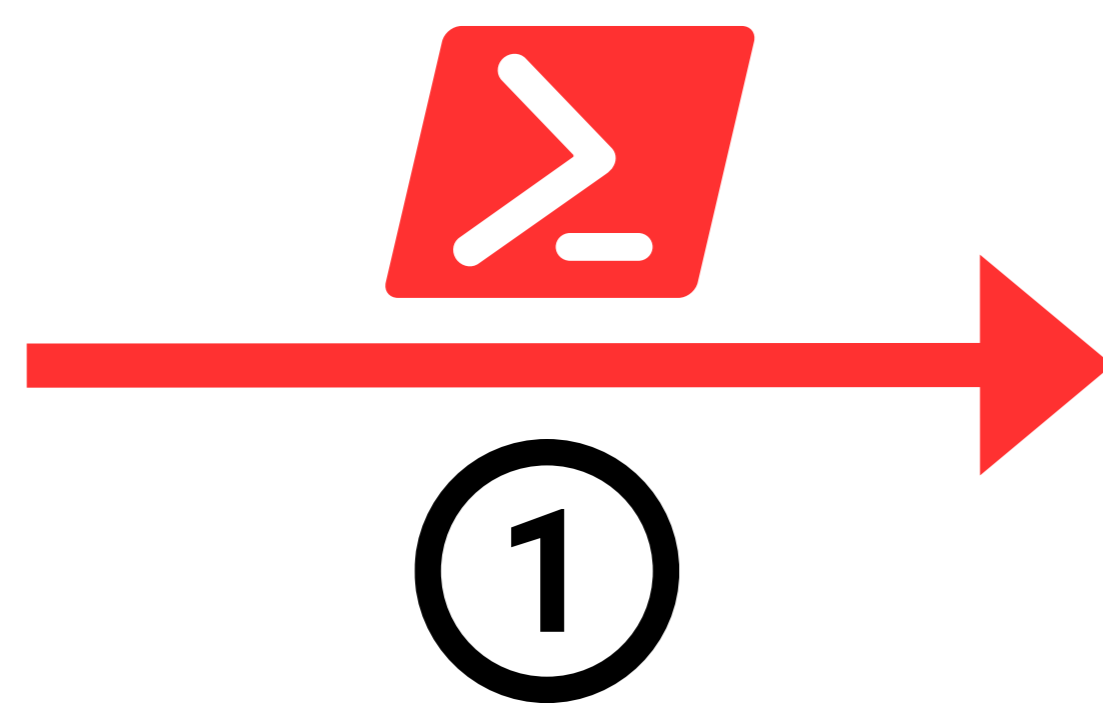
Уязвимый сайт

веб-сервер

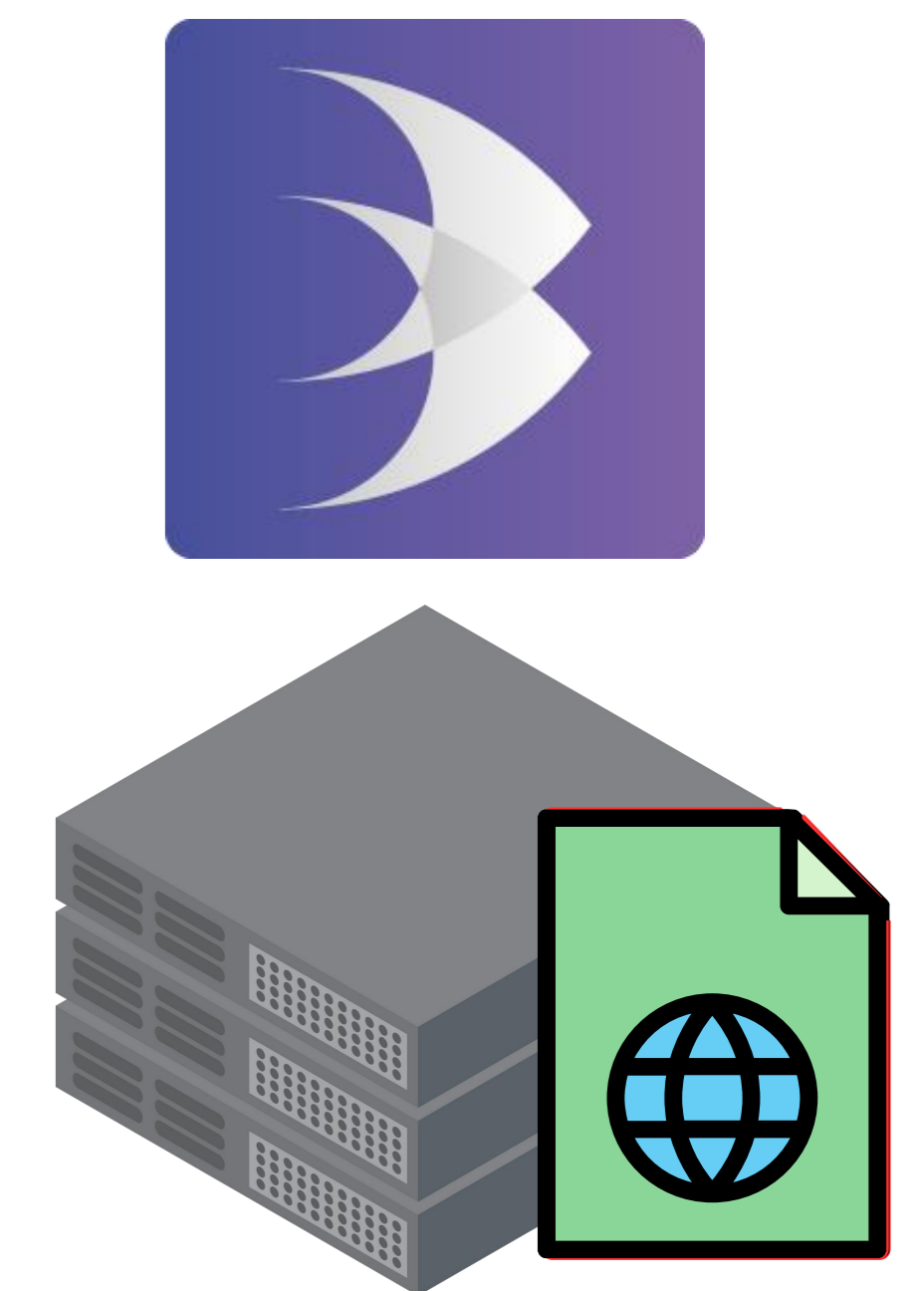


# Как работает WARSS?

Уязвимый сайт



веб-сервер



# Демонстрация

The screenshot displays the WARSS 2.7.0.4 interface. The main terminal window shows the following commands and output:

```
[root@localhost html]# ll
total 4432
-rw-r--r--. 1 root root 279 Jun 11 05:58 index_2.html
-rw-r--r--. 1 root root 281 May 31 04:14 index.html
-rw-r--r--. 1 root root 1682529 Jun 11 05:24 resim1.png
-rw-r--r--. 1 root root 2844197 Jun 11 05:24 resim2.png
drwxr-xr-x. 2 root root 42 Jun 11 07:51 warss1
drwxr-xr-x. 2 root root 42 Jun 25 08:14 warss2
[root@localhost html]# cp -R index_2.html warss1/index.html
cp: overwrite 'warss1/index.html'? y
[root@localhost html]# cp resim2.png warss1/
[root@localhost html]# cp -R index_2.html warss2/index.html
cp: overwrite 'warss2/index.html'? y
[root@localhost html]# cp resim2
```

The Monitor window on the right shows the following settings and logs:

**Settings:**

- Anti-Falsification Detection
- Warnings
- Agent Status
- Detection Errors
- Network Status

**Log Table:**

Contents	Agent Name	Server Name
The Restore Anti-Falsification file has been rest...	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Network connected.	(1) localhost.locald...	WARSS

<https://www.youtube.com/watch?v=B20LDk0iAJO>

# Конфигурация WARSS



## WARSS Management Server(s)

- Серверное программное обеспечение, установленное на аппаратном обеспечении/виртуальной машине
- Удаленное управление и контроль агентов
- Сохраняет историю обнаружений
- Распространяет обновления и изменения настроек среди агентов



## WARSS Agent(s)

- Программа установлена на веб-сервере/WAS
- Обнаруживает изменения файлов
- Совместимость с Unix, Linux, Windows NT O/S (должна поддерживаться JDK 1.5+)



## WARSS Manager Program

- Программа, установленная на компьютере администратора
- Управление настройками для: обнаружения, удаленного действия, среды и отчетности
- Настройки управления доступом, статистики и отчетности

# Чем отличается WARSS

## WARSS



## Web Crawlers



**Метод обнаружения:**

**В режиме реального времени,**  
На основе шаблонов

**Периодическое** обнаружение

**Загрузка:**

**Оптимизированное** использование  
ресурсов (~1% ЦП)

**Без агента**

**Цель обнаружения:**

**Серверные файлы** (исходный код,  
данные, содержимое)

Скомпилированные единицы  
измерения URL и файлы данных

**Смягчение:**

**Автоматическое восстановление в**  
**режиме реального времени**

**Ручное устранение последствий**  
при нарушении



# Обнаружение в режиме реального времени

Защита исходного кода и содержимого



Легковесный

Немедленная реставрация и восстановление

# Нулевое доверие

1. “Никогда не доверяй, всегда проверяй”
2. Доступ с минимальными привилегиями
3. Предполагаемое нарушение

# Нулевое доверие

## 3. Предполагаемое нарушение



**Доступность**  
Информация доступна  
по мере необходимости



**Конфиденциальность**

Информация доступна  
только авторизованным  
лицам



**Целостность**  
Информация точна и  
защищена от  
искажений

# Соответствие ISO/IEC 27001

Применимые требования:

- 8.1** Операционное планирование и контроль
- 8.3** Обработка рисков информационной безопасности
- 9.1** Мониторинг, измерение, анализ и оценка



# Соответствие ISO/IEC 27001

## Применимые технологические контроли

- 8.4** Доступ к исходному коду
- 8.6** Управление емкостью
- 8.7** Защита от вредоносных программ
- 8.8** Управление техническими уязвимостями
- 8.12** Предотвращение утечек данных
- 8.13** Резервное копирование информации
- 8.15** Журналирование
- 8.16** Мониторинг деятельности
- 8.23** Веб-фильтрация
- 8.26** Требования к безопасности приложений



# Сертифицирован по уровню 1 GS (Good Software)

- Тестовые стандарты:  
ISO/IEC 25023, 25051, 2504
- Протестировано на:
  - Функциональную пригодность
  - Эффективность производительности
  - Совместимость
  - Удобство использования
  - Надежность
  - Безопасность
  - Обслуживаемость
  - Портативность



# Примеры использования



# Государственное оборонное учреждение

## Недостатки безопасности

Недовольны производительностью и удобством управления веб-ориентированного программного обеспечения для обнаружения подделок 'W'

## Их чек-лист

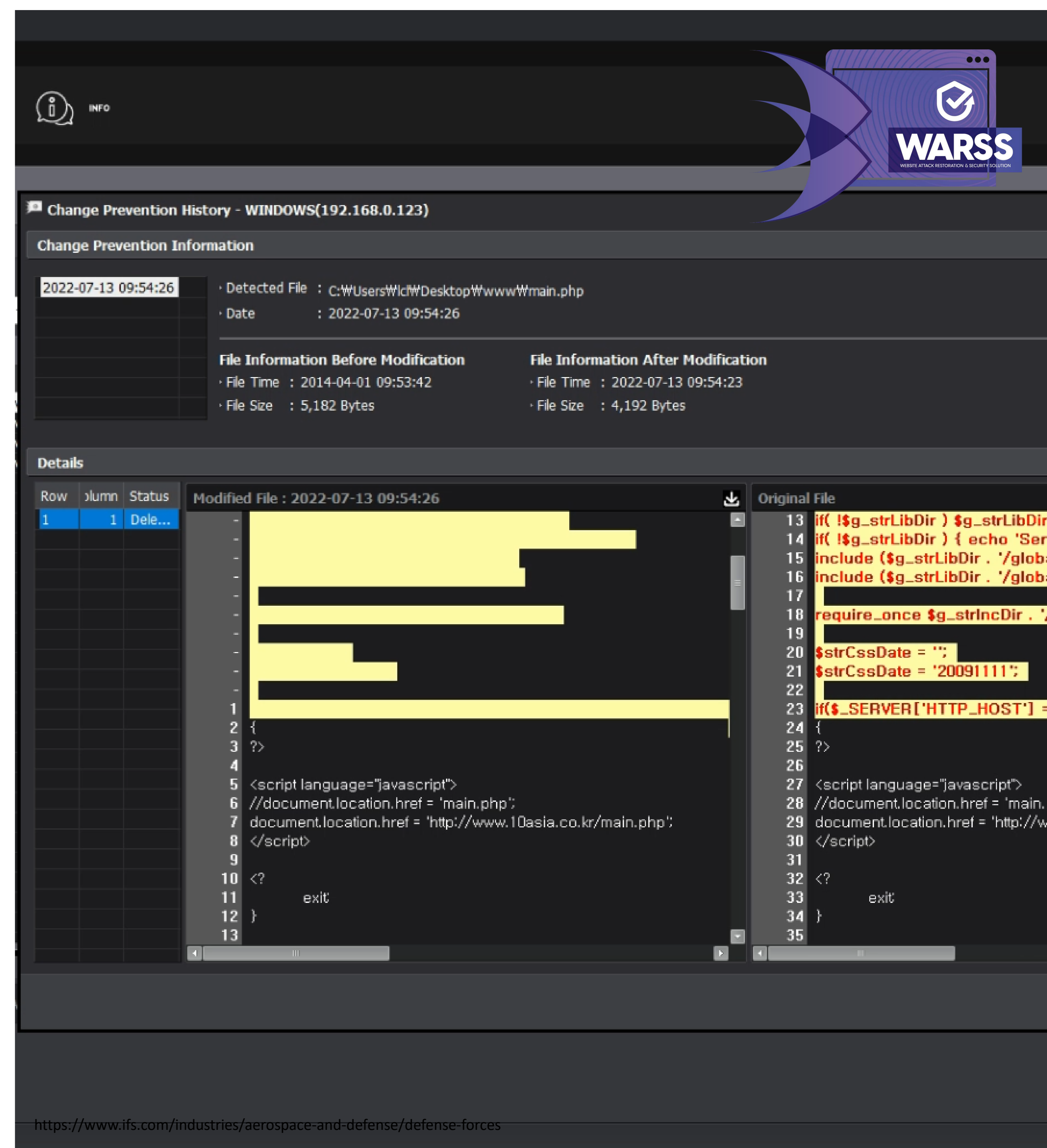
Они искали агентское решение, которое предлагало бы автоматическое восстановление и эффективное управление

## "Реализация WARSS в 2023 году

Установили 50 агентов WARSS на всех веб-серверах

## Их отзывы

Восторженно отзывались о функции автоматического обнаружения домашнего каталога в WARSS, которая позволяет легко настраивать обнаружение без необходимости вручную вводить URL



<https://www.ifs.com/industries/aerospace-and-defense/defense-forces>

# Транспортное агентство

## Беспокойства по поводу подделки контента

Работающий веб-сайт с образовательным контентом (изображения, видео); попытка и неудача в аутсорсинге разработки собственной решения против подделок

## Почему WARSS?

По сравнению с другими решениями против подделок, которые они тестировали, WARSS был единственным, который предложил защиту от подделки исходного кода, изображений и видео

## Почему они выбрали WARSS?

Установили 100 агентов WARSS на все веб-серверы

## Непрерывная защита

С тех пор WARSS предотвращает любые случаи подделок; клиент продолжает покупать Агентов каждый раз, когда добавляет серверы в свою систему

The screenshot displays the WARSS (Web Application Runtime Security Solution) interface. At the top right, the WARSS logo is visible. The main window shows 'Change Prevention History - WINDOWS(192.168.0.123)'. Below this, there's a section for 'Change Prevention Information' with a table listing detected files. One entry is highlighted: '2022-07-13 09:54:26' for a file at 'C:\Users\Wlc\Desktop\www\main.php' detected on '2022-07-13 09:54:26'. Below the table, there are two columns: 'File Information Before Modification' (File Time: 2014-04-01 09:53:42, File Size: 5,182 Bytes) and 'File Information After Modification' (File Time: 2022-07-13 09:54:23, File Size: 4,192 Bytes). The bottom section, 'Details', shows a side-by-side comparison of the file's content. The 'Modified File' column shows a JavaScript script with a redacted section. The 'Original File' column shows the original code, including a conditional statement for the server's host name: `if($_SERVER['HTTP_HOST'] = ...)`.

<https://www.globaltranz.com/resource-hub/transportation-terminology/>

# Кто использует WARSS?

WARSS защищает репутацию нескольких национальных компаний и учреждений.



... и многое другое!

# СОТНИ КЛИЕНТОВ

Продукты UMV обеспечивают безопасную и стабильную защиту веб-серверов сотен клиентов более десяти лет.



13+ years



13+



7-8



13+



10+



13+



... и многое другое!



**umv**

# Спасибо вам!

## Свяжитесь с нами

**UMV Inc.**

Сеул, Южная Корея



+82 2 448 3435



sales@umvglobal.com



www.umvglobal.com

**UMV Kaz**

Алматы, Казахстан



+7 700 980 7428



sales@umvglobal.com



www.umvglobal.com

# Приложение

# Функции WARSS

## Обнаружение подделок и восстановление

Название Функции	Описание
Обнаружение подделок	Обнаружение и уведомление о подделке и изменении исходных файлов и данных веб-сайта
Восстановление после подделки	Восстановление оригинальных файлов в реальном времени при обнаружении подделки
Переназначить оригинал	Переназначить базовые/оригинальные файлы, когда необходимо внести законные изменения

# Представление обнаружения подделок

Обнаружение подделок и восстановление в реальном времени

The screenshot displays the WARSS 2.5.8 Anti-Forgery interface. The main window shows a list of detected files with the following columns: Report Date and Path. The detected file is:

Report Date	Path
2022-07-13 09:54:26	C:\Users\Wic\Desktop\www\main.php
2022-07-13 09:53:58	C:\Users\Wic\Desktop\www\main.php
2022-07-13 09:53:58	C:\Users\Wic\Desktop\www\main.php
2022-07-13 09:53:58	C:\Users\Wic\Desktop\www\main.php

The 'Change Prevention History - WINDOWS(192.168.0.123)' window is open, showing the following information:

**Change Prevention Information**

- 2022-07-13 09:54:26
- Detected File : C:\Users\Wic\Desktop\www\main.php
- Date : 2022-07-13 09:54:26

**File Information Before Modification**

- File Time : 2014-04-01 09:53:42
- File Size : 5,182 Bytes

**File Information After Modification**

- File Time : 2022-07-13 09:54:23
- File Size : 4,192 Bytes

The 'Details' window shows a comparison between the 'Modified File' and the 'Original File'. The modified file contains a JavaScript script that attempts to redirect the browser to a different domain. The original file contains a PHP script that checks the server environment and includes other files.

```
Modified File : 2022-07-13 09:54:26
1
2 {
3 }
4
5 <script language="javascript">
6 //document.location.href = 'main.php';
7 document.location.href = 'http://www.10asia.co.kr/main.php';
8 </script>
9
10 <?
11     exit
12 }
13

Original File
13 if( !$g_strLibDir ) $g_strLibDir = '/app/aknsys/phplib';
14 if( !$g_strLibDir ) { echo 'Server Env Var not define'; exit( 0
15 include ( $g_strLibDir . '/global_var.inc.php' );
16 include ( $g_strLibDir . '/global_func.inc.php' );
17
18 require_once $g_strIncDir . '/10asia/lib/_VCONFIG.php';
19
20 $strCssDate = '';
21 $strCssDate = '20091111';
22
23 if($_SERVER['HTTP_HOST'] == 'www.10-magazine.com' || !
24 {
25 }
26
27 <script language="javascript">
28 //document.location.href = 'main.php';
29 document.location.href = 'http://www.10asia.co.kr/main.php';
30 </script>
31
32 <?
33     exit
34 }
35
```



# Функции WARSS

## Управление

Название Функции	Описание
Управление обновлениями	Обновления агентов и менеджеров, управление версиями
Управление правами доступа и отчетностью	<ul style="list-style-type: none"><li>• Управление правами доступа по учетным записям и пользователям</li><li>• Взаимодействие с внешними системами (ESM, SMS, E-mail и т.д.)</li><li>• Отчеты и статистика</li></ul>
Стабильность	<ul style="list-style-type: none"><li>• Контроль использования ресурсов</li><li>• Настройка в соответствии с серверной средой</li></ul>
Обнаружение IP-адреса атакующего	Отчеты по IP-адресам выполнения для поддельных файлов (доступно, когда активирована только функция обнаружения)
Управление предпочтениями	Управление конфигурационными файлами веб-сервера/WAS и настройки обнаружения изменений
Выделенный безопасный загрузчик	<ul style="list-style-type: none"><li>• Указание безопасного каталога загрузки для каждой учетной записи пользователя</li><li>• Проверка наличия вредоносного кода в файлах, загруженных с использованием безопасного загрузчика</li></ul>



# Вид управления

## Права администратора

Manage Admin

ShellMonitor-1 (192.168.0.119)

Administrator List

Admin Authority

Agent Authority for Admin

Agent Authority for Agent

Upload Properties

Message Settings

### Authorizations

Authority Level	Authority
<input type="checkbox"/> Super Administrator	<input type="checkbox"/> Agent - Process Detections
<input type="checkbox"/> Intermediate Administrator	<input type="checkbox"/> Agent - Settings (General, WAS)
<input type="checkbox"/> General Administrator	<input type="checkbox"/> Agent - Settings (Detection Rules)
<input type="checkbox"/> Control Operator - Multi	<input type="checkbox"/> Agent - Pause/Restart
<input type="checkbox"/> Control Operator - Single	<input type="checkbox"/> Agent - Update Pattern Manually
	<input type="checkbox"/> Server - Use Multi-Server
	<input type="checkbox"/> Server - Settings
	<input type="checkbox"/> Create Admin Account
	<input type="checkbox"/> Agent Allocation, Create Group
	<input type="checkbox"/> File Upload
	<input type="checkbox"/> Message Settings
	<input type="checkbox"/> Delete Agent

Add Delete

Apply

# Вид управления

## Стабильность

(1)localhost.localdomain ×

Settings ShellMonitor-1 > Unassigned > (1)localhost.localdo...

General | WAS | File Detection | Upload Filtering | Malicious URL List | Local Pattern List | Advanced

Server Access Settings View More

Web Server Safeguard Server Address : 192.168.0.122 Port : 7778  
Upload Server Address : 192.168.0.122 Port : 7777  
Detection File Management Server Address : Port : 0

General Settings

Detection Settings

CPU Usage Limit :  10  
Issue alert if Agent CPU usage exceeds  %  
System CPU Usage  %

Update Settings

Pattern Updates :  Manual  
 Automatic (Before Detecting)  
 Periodic  at  minute(s) past

No full detecting when updating global pattern

Reset Apply

# Вид управления


Мониторинг состояния ресурсов

(2)localhost.localdomain ×

Information ShellMonitor-1 > Unassigned > (2)localhost.localdo...


Agent Information | System Information | **Resource Status** | Docker Information | Docker Container Information

### Agent CPU Usage




Agent CPU Usage : 0.0%

### System CPU Usage



System CPU Usage : 0.2%

### Memory



Physical Memory	Virtual Memory	Hard Disk
Usage Rate : 38.7%	Usage Rate : 17.9%	Usage Rate : 3.6%
Total : 3665.7MB	Total : 196.5MB	Total : 24.6GB
Used : 1420.5MB	Used : 35.3MB	Used : 0.9GB
Available : 2245.2MB	Available : 161.2MB	Available : 23.7GB

# Вид управления

## Обнаружение IP-адреса атакующего

Attacker IP Detection □ ×

Access Log List ( Total 0 )

WAS	Acces Log Path	Configuration File	Directory

Access Log List ( Total 0 )

Status	File

Agent List

Delete Apply Close

# Вид управления

## Управление предпочтениями

(2)localhost.localdomain ×

Settings ShellMonitor-1 > Unassigned > (2)localhost.localdo...

General | WAS | **File Detection** | Upload Filtering | Malicious URL List | Local Pattern List | Advanced

**Basic Detection Settings** General

Real-Time Monitoring :  On

Execution Cycle : None

Rescan :  On CPU Usage Limit :  10

Forgery :  Detection  Bytes  Recover

Malicious URL Detection :  On  Assign to White List for Full Detections

Personal Information Detection :  On (  Social Security Number  Alien Registration Number  Individual Business Registration Number  Mobile Phone Number  Phone Number  Account Number  Card Number  E-Mail  Driver's License Number  Health Insurance Number  Passport Number )

Countries subject to personal information detection : Korea

Backup Policy :  Detected WebShells  Detected WebShells & Changed Files  Personal Information Detection File Backup

No. of Backup Files :  Send notification when number of detection files exceeds :

BackUp Clearing Settings :  Time-Based BackUp Auto-Clear  Day(s)

Automatic Quarantine :  Well-Known WebShells  Encoding  Black List URLs  Hash

Detect Well-Known WebShells Only :  On Detect Extension Bypasses :  On

Archive File Detection :  On Send notification when elapsed time since detected files was last checked exceeds :  Hour(s)

Limit Detection File Size :  KByte(s) Pause When Total Memory Usage Exceeds 95% :  On

Limit Forgery File Size :  KByte(s) Hash Detection :  On

**Detection Directory Settings** ( Total 0 )

On	Directory	Status	adabl	Writable	etting:	Code	Forgery	ecove	Extensions	URL

# Вид управления

Выделенный безопасный загрузчик

**Manage File Uploads** ShellMonitor-1 (192.168.0.119)

**Agent List** Removing Recovery

3-Tier 2-Tier

- All
  - Unassigned
    - (1) localhost.localdomain
    - (2) localhost.localdomain **Connect**

**Upload Target**

- C:
  - \$Recycle.Bin
  - \$WINRE\_BACKUP\_PARTITION.MARKER
  - %AMBU9P
  - @\$SDSEV
  - adobeTemp
  - Documents and Settings
  - DumpStack.log
  - DumpStack.log.tmp
  - for local
  - hiberfil.sys
  - pagefile.sys
  - Program Files

**Admin Edit Permission Paths** Set for Recovery Remove from Recovery

Class	Path
-------	------

Path :

Settings Delete Apply



# Функции WARSS

## Поддержка облачных вычислений

Названия Функции	Описание
Масштабирование внутри/внешне	<ul style="list-style-type: none"><li>• Автоматическая регистрация новых целей обнаружения при масштабировании; обнаружение начинается автоматически</li><li>• Автоматические резервные копии журналов обнаружения/изменений/удалений на сервер управления для удаленных агентов при масштабировании</li></ul>
Поиск в домашнем каталоге	<ul style="list-style-type: none"><li>• Запланировать обнаружение изменений/добавлений в домашний каталог веб-сервера/WAS</li><li>• Просмотр истории добавлений/изменений в домашнем каталоге</li></ul>
Управление историей	Управление состоянием и историей работы агентов (установка, удаление, запуск/остановка и т.д.)
Предотвращение дублирования событий	Предотвращение дублирования событий обнаружения в избыточных системах, когда домашний каталог включен в область NAS

# Просмотр настроек облака

Поиск в домашнем каталоге

The screenshot displays a web interface for configuring cloud settings. The main window is titled '(2)localhost.localdomain' and contains various configuration options such as 'Real-Time Monitoring', 'Execution Cycle', 'Forgery', 'Malicious URL Detection', and 'Personal Information Detection'. A modal window titled 'Anti-Forgery Detection Directory Settings - localhost.localdomain(192.168.0.119)' is open, showing a table with a 'Path' column and a '( Total 0 )' count. The modal also includes radio buttons for 'Include in Anti-Forgery Detection' (selected) and 'Exclude From Recovery'. At the bottom of the modal are buttons for 'Directory Settings', 'Delete', and 'Apply'. The main interface also features a 'Reset' button and an 'Anti-Forgery Detection Directory Settings' button with an 'Apply' sub-button.

Real-Time Monitoring :  On

Execution Cycle : None

Rescan :  On CPU Usage Limit : 10

Forgery :  Detection

Malicious URL Detection

Personal Information Detection

Countries subject to personal info

Backup Policy

No. of Backup Files

BackUp Clearing Settings

Automatic Quarantine

Detect Well-Known WebShells On

Archive File Detection

Limit Detection File Size

Limit Forgery File Size

**Detection Directory Settings**

On	Directory
----	-----------

Anti-Forgery Detection Directory Settings - localhost.localdomain(192.168.0.119)

Include in Anti-Forgery Detection  Exclude From Recovery ( Total 0 )

Path
------

Directory Settings Delete Apply

Reset

Anti-Forgery Detection Directory Settings Apply

# Просмотр настроек облака

Управление журналами/историей

The screenshot shows the 'Monitor' application window. At the top, there are several filter checkboxes: 'Anti-Falsification Detection', 'Warnings', 'Agent Status', 'Detection Errors', and 'Network Status', all of which are checked. Below these, there are radio buttons for 'Today' (selected) and 'Specify Period'. Under 'Specify Period', there are two date input fields, both containing '25.06.2024', separated by a tilde '~'. A blue 'Search' button is located to the right of the date fields. Below the filters is a table with three columns: 'Contents', 'Agent Name', and 'Server Name'. The table contains ten rows of data, all with a yellow background color. The 'Contents' column lists various events such as 'Settings file changed.', 'Agent set not to detect.', and 'Network connected.'. The 'Agent Name' column shows '(1) localhost.locald...' for all entries. The 'Server Name' column shows 'WARSS' for all entries.

Contents	Agent Name	Server Name
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Settings file changed.	(1) localhost.locald...	WARSS
Agent set not to detect.	(1) localhost.locald...	WARSS
Network connected.	(1) localhost.locald...	WARSS

# Диаграмма конфигурации WARSS On-Premise

